IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
AMARILLO DIVISION

ROLANDO CRUZ LOPEZ and JAMES FOXE, Plaintiffs, v. ALEJANDRO PENA, individually; UNITED STATES CUSTOMS AND BORDER PROTECTION; UNITED STATES DEPARTMENT OF HOMELAND SECURITY Defendants.	§ § § § § § § § § § § § §	No. 2-12-CV-165-J

MEMORANDUM AND ORDER

Before the Court is Defendant Alejandro Pena's *Motion to Dismiss Count II of the Amended Complaint*, filed April 4, 2013. In Count II as amended, pro se Plaintiff Rolando Cruz Lopez claims that Pena, in his individual capacity as a Customs and Border Protection (CBP) agent, violated the Stored Communications Act (SCA), 18 U.S.C. §§ 2701(a) and 2703, by accessing Cruz Lopez's Yahoo! email account. Pena asserts that qualified immunity precludes these claims because his alleged access of Cruz Lopez's account did not violate any clearly established right in the SCA. Pena's motion will be granted as to § 2701(a) but denied as to § 2703.

BACKGROUND

Count II—the only count remaining against Pena—stems from an August 8–9, 2009 incident at the Dallas/Fort Worth International Airport during which Pena and other CBP officers detained Cruz Lopez en route to visit Plaintiff James Foxe in Amarillo. Pena allegedly found usernames and passwords in Cruz Lopez's wallet and then accessed Cruz Lopez's online bank account, Yahoo! email account, and possibly his Hotmail account. Pena executed an expedited

removal order against Cruz Lopez for supposedly working in the United States as Foxe's employee in violation of visa restrictions.

Cruz Lopez claims that he discovered, in a January 2012 FOIA disclosure, that Pena had accessed at least six emails from his Yahoo! account: (1) a message sent to Cruz Lopez by an acquaintance on May 8, 2009; (2) and (3) Cruz Lopez's May 15 responses to the May 8 message; (4) the acquaintance's May 18 response to at least one of Cruz Lopez's May 15 responses; (5) Cruz Lopez's June 27 response to the acquaintance's May 18 response; and (6) Cruz Lopez's July 4 response to the acquaintance's May 18 response. Cruz Lopez also alleges that Pena may have accessed other emails, including unopened messages.

The Court dismissed Cruz Lopez's original Count II but granted leave to amend. Docket #37. Cruz Lopez now claims that Pena violated § 2701(a) of the SCA by accessing, without permission, emails that were in electronic storage. He also claims that Pena violated § 2703 by compelling the disclosure of electronic communications from Yahoo! without a warrant, subpoena, or court order. He seeks actual and punitive damages, fees and costs. These sections are made civilly actionable by § 2707.

LEGAL STANDARD

A motion to dismiss based on qualified immunity is generally evaluated under the Rule 12(b)(6) rubric. *See Collins v. Ainsworth,* 382 F.3d 529, 536 (5th Cir. 2004); *Baker v. Putnal,* 75 F.3d 190, 197 (5th Cir. 1996); *Richard v. Capps,* 2007 WL 2428928, at *2 n.6 (N.D. Tex. Aug. 28, 2007).

In determining motions for failure to state a claim, the Court first identifies allegations not entitled to the assumption of truth due to their lack of factual support and then assumes the veracity of the remaining non-fanciful alleged facts. *Ashcroft v. Iqbal*, 556 U.S. 662, 664 (2009).

The Court then denies the motion to dismiss if the complaint "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570).

When an official is sued in his individual capacity, however, a modification to the basic Rule 12(b)(6) standard applies. The official's qualified immunity defense fails only if the complaint, with "factual detail and particularity," states facts plausibly alleging that the official, engaging in objectively unreasonable conduct, (1) violated a constitutional or statutory right that (2) was at the time, and still is, clearly established. *Anderson v. Pasadena Indep. Sch. Dist.*, 184 F.3d 439, 443 (5th Cir. 1999) (citing *Jackson v. Widnall*, 99 F.3d 710, 715–16 (5th Cir. 1996)); *see Morgan v. Swanson*, 659 F.3d 359, 371–72 (5th Cir. 2011).

QUALIFIED IMMUNITY

Cruz Lopez's § 2701(a) Claim

Section 2701(a) of the SCA protects electronic communications while in electronic storage and is made civilly actionable by § 2707.

Testing qualified immunity, the Court asks whether the complaint contains sufficient facts to plausibly show that, by objectively unreasonable conduct, (1) Pena violated a right in § 2701(a) that (2) was clearly established in August 2009 and still is. *See Morgan*, 659 F.3d at 371–73; *Kipps v. Caillier*, 197 F.3d 765, 768 (1999); *Bazan ex rel. Bazan v. Hidalgo County*, 246 F.3d 481, 490 (5th Cir. 2001).

Section 2701(a) creates a right against anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or

prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a).

"Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

Cruz Lopez argues that some of the six emails Pena allegedly accessed were in electronic storage incident to transmission. Emails not yet opened by the intended recipient are in such storage. *See* Order, Docket #37 at 6–7. But none of the six emails Cruz Lopez accuses Pena of accessing were unopened: Cruz Lopez must have opened the first email because he responded to it; *he* sent the second and third emails, and it is not clearly established that sent communications are in electronic storage when accessed from the sender's account, *see, e.g.*, *United States v. Weaver*, 636 F. Supp. 2d 769, 769–70 (C.D. Ill. 2009) (enforcing subpoena that called sent mail "communications not in electronic storage"); he obviously opened the fourth because he responded to it; and the fifth and sixth have the same problem as the second and third. None of the emails is adequately alleged to have been in electronic storage on August 8–9, 2009.

Cruz Lopez's allegation that Pena *might* have accessed unopened emails either in Cruz Lopez's Yahoo! or Hotmail account is unavailing. Its bare equivocation falls short of the factual detail and particularity necessary to overcome qualified immunity. *Anderson*, 184 F.3d at 443.

Because the allegations in the complaint are inadequate, discovery is inappropriate. *See Wicks v. Miss. State Employment Servs.*, 41 F.3d 991, 994 (5th Cir. 1995). Cruz Lopez's § 2701(a) claim is dismissed.

Cruz Lopez's § 2703 Claim

"A governmental entity may require a provider" of a remote computing service or electronic communication service "to disclose the contents of any . . . electronic communication" if the governmental entity obtains a warrant, subpoena, or court order, depending on the circumstance. 18 U.S.C. § 2703.

Is it clearly established that a governmental entity violates § 2703 by hacking into a user's online email account instead of seeking a warrant, subpoena, or court order? Pena notes that no Fifth Circuit or Supreme Court case addresses this question. Cruz Lopez is correct, however, that the standard to determine clearly established law is whether "in the light of pre-existing law the unlawfulness [is] apparent," *Hope v. Pelzer*, 536 U.S. 730, 739–40 (2002), not whether a prior case is directly on point. A statute might be sufficiently unambiguous to prove apparent unlawfulness on its own, without a court's prior say-so. The SCA is famous for its lack of clarity, but what Pena allegedly did obviously violates § 2703.

"[T]he *only* procedure available to [law enforcement] to obtain 'disclosure' of the contents of electronic communications [i]s to comply with this statute." *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 816 F. Supp. 432, 443 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994) (emphasis added). Under § 2701, law enforcement officers are normally barred from accessing a user's electronic communications that are in electronic storage because they are not authorized to access those communications. As noted above, § 2701 provides no recourse against someone accessing communications that are *not* in electronic storage. Section 2703, on the other hand, procedurally safeguards all electronic communications in a provider's possession. Unless authorized, a law enforcement officer must follow § 2703 procedures to get a user's electronic communications from the provider.

Yahoo! is a provider under § 2703 and Yahoo! automatically disclosed the emails when Pena logged on, so Pena is left arguing that § 2703 is inapplicable as it applies only to *required* disclosure (what he calls compelled disclosure), and he did not require Yahoo! to do anything because Yahoo! willingly provided access to the account. It is true that a governmental entity following § 2703 "may require" a provider to disclose electronic communications. But it is not true that an officer can ignore § 2703 procedures, hack into an account, and then claim that § 2703 is inapplicable because the provider thought that the officer was the user. *Cf. Freedman v. Am. Online, Inc.*, 303 F. Supp. 2d 121, 127 (D. Conn. 2004) (holding that officers violated § 2703 even though provider complied with invalid warrant).

The most common definition of require is "to claim or ask for by right and authority." *Merriam Webster's Collegiate Dictionary* (11th ed. 2003). Cruz Lopez's complaint sufficiently alleges that Pena, posing as one with the right and authority to do so, sought disclosure of Cruz Lopez's emails by entering the correct username and password and clicking "sign in." Pena's actions apparently required Yahoo! to disclose whatever messages were in Cruz Lopez's account, contrary to Pena's argument that he did not require disclosure but merely accessed Yahoo!'s facility.

To the extent that require means to compel against one's will, Pena cannot say that Yahoo! willingly turned over Cruz Lopez's emails to law enforcement. Pena's posing as Cruz Lopez shows, at best, that if Pena did not compel Yahoo! to unwillingly disclose to law enforcement, he is at least alleged to have tricked Yahoo! to unwittingly disclose.

An officer violates § 2703 by seeking that section's ends without following its procedures. That is what Cruz Lopez alleges: Pena wanted to find some basis for expedited removal of Cruz Lopez but was not authorized to log onto Cruz Lopez's Yahoo! account, so,

instead of following § 2703, he hacked in and took what he wanted. Pena points out that he did not interact with Yahoo! personnel by submitting a paper request for particular communications, but that is Cruz Lopez's point: if § 2703 is violated when an officer uses an incomplete warrant application to seek disclosure, *see Freedman*, 303 F. Supp. 2d at 127, then § 2703 is even more clearly violated when an officer requires the provider to give up communications *without* any subpoena, warrant, or court order. Pena is adequately alleged to have violated § 2703's clear mandate that an officer not require a provider to disclose communications without statutory process.

CONCLUSION

Pena's motion to dismiss the § 2701 claim is GRANTED with prejudice. Pena's motion to dismiss the § 2703 claim is DENIED.

It is SO ORDERED.

Signed this the 22nd day of May, 2013.

MARY LOU ROBINSON
UNITED STATES DISTRICT JUDGE